Scientific Bulletin of the „Petru Maior" University of Tîrgu Mureş
Vol. 11 (XXVIII) no. 1, 2014
ISSN-L 1841-9267 (Print), ISSN 2285-438X (Online), ISSN 2286-3184 (CD-ROM)

ENABLING SOFTWARE DEFINED NETWORKING EXPERIMENTS IN NETWORKED CRITICAL INFRASTRUCTURES

Béla GENGE[1], Zoltán GÁL[2]

[1] *"Petru Maior" University of Tîrgu Mureş*
Nicolae Iorga Street, no.1, 540088, Tîrgu Mureş, Romania
[1]bela.genge@ing.upm.ro
[2]*University of Debrecen*
Egyetem tér 1, Debrecen, Hungary, 4032
[2]zgal@unideb.hu

Abstract

Nowadays, the fact that Networked Critical Infrastructures (NCI), e.g., power plants, water plants, oil and gas distribution infrastructures, and electricity grids, are targeted by significant cyber threats is well known. Nevertheless, recent research has shown that specific characteristics of NCI can be exploited in the enabling of more efficient mitigation techniques, while novel techniques from the field of IP networks can bring significant advantages. In this paper we explore the interconnection of NCI communication infrastructures with Software Defined Networking (SDN)-enabled network topologies. SDN provides the means to create virtual networking services and to implement global networking decisions. It relies on OpenFlow to enable communication with remote devices and has been recently categorized as the "Next Big Technology", which will revolutionize the way decisions are implemented in switches and routers. Therefore, the paper documents the first steps towards enabling an SDN-NCI and presents the impact of a Denial of Service experiment over traffic resulting from an XBee sensor network which is routed across an emulated SDN network.

Key words: software defined networking, networked critical infrastructures, industrial control systems, OpenFlow, Floodlight, Mininet, SDN

1. Introduction

The adoption of Commodity Of The Shelf (COTS) hardware and software in the architecture of modern Networked Critical Infrastructures (NCI) created a novel palette of features and capabilities. The high penetration of these devices even within the core of NCI paved the way for service interoperability, interconnection of networks, remote monitoring and control, new financial services, as well as the newly emerging Smart Grid.

These large-scale infrastructures deployed across city, regional, national or even over international geographical areas provide the basic services that our society depends on. Consequently, the disturbance of their normal functionality either from natural causes, malfunctioning, or cyber attacks can have a "serious impact on the health, safety, security or economic well-being of citizens" [3]. Taking for instance the example of the next electricity grid, nowadays known as *Smart Grid*, it is foreseen that the deployment of large-scale Smart Grids will provision several indisputable advantages and benefits, e.g., improved operational benefits of control, reliability and safety, advanced two-way communications, and more flexible integration of heterogeneous measurement and sensor-actuator networks. Nevertheless, recent incidents and scientific research has shown that these are also being exposed to significant risks [10], [1]. The discovery of the Stuxnet [2] malware, the world's first (discovered) malware capable to rewrite the control logic of Industrial Control Systems (ICS) hardware, marked a turning point in how cyber security specialists view the security of these infrastructures. Subsequently, the potential impact of cyber attacks in the power sector has been highlighted by the Tempe, AZ incident [15] from 2007. In this particular case an improper configuration of load shedding programs caused the opening of 141 breakers and a loss of significant load, which subsequently led to a 46 min power outage affecting almost 100 000 customers.

In this context the deployment of effective protective mechanisms and the adoption of novel techniques to mitigate attacks are considered an international priority. In this paper we explore the applicability of Software Defined Networking (SDN) [13] in the implementation of security experiments for NCI. SDN is a newly emerging trend which intends to replace switch-based configurations with an external software control pane, leading to more flexible and highly dynamic routing decisions.

The approach described in this paper combines in a unique way different experimentation capabilities in order to enable experimentation with SDN-based networks, Smart Grid-specific protocols, as well as a wide variety of sensor networks. The paper documents the first steps towards enabling an SDN-NCI and presents the impact of a Denial of Service experiment over traffic originating from an XBee sensor network which is routed over an emulated SDN network.

The remaining of this paper is organized as follows: Section 2 provides an overview of related work, emphasizing at the same time the novelty and significance of the work beforehand; Section 3 provides an overview of the proposed approach for enabling SDN experiments in NCI; Section 4 provides experimental results consisting of a real sensor network recreated with MaspMote and Meshlium modules; the paper concludes in Section 5.

2. Related work

The possible impact of cyber attacks on the normal functioning of NCI and finally on society, have brought the topic of NCI security in the attention of academia, industry and policy makers. As such, today we find a wide range of theoretical approaches, recommendations and practical solutions to secure NCI assets.

The National Institute of Standards and Technology's (NIST) "Guide to Industrial Control Systems" [12] provides a wide range of techniques and best practices to enhance the security of ICS. Defense-in-depth is strongly recommended in order to provide multiple layers of defense and detection. Network segmentation combined with correctly configured firewalls can raise significant barriers in the path of cyber attackers.

State-of-the-art IP networking solutions can bring significant advantages in the mitigation of attacks. Internet Protocol/Multi-Protocol Label Switching (IP/MPLS) provides the ability to define virtual circuits and separate routing tables [5], [8]. Different traffic flows can be separated and QoS-based techniques can be applied in order to reduce the interference of different flows [5].

Intrusion/anomaly detection systems also represent an important line of proactive defense strategy in the architecture of NCI. Recent advancements in the field of NCI security highlighted the advantages of anomaly detection techniques to efficiently detect abnormal behavior [7], [6], [14], [16], [4] in the context of NCI.

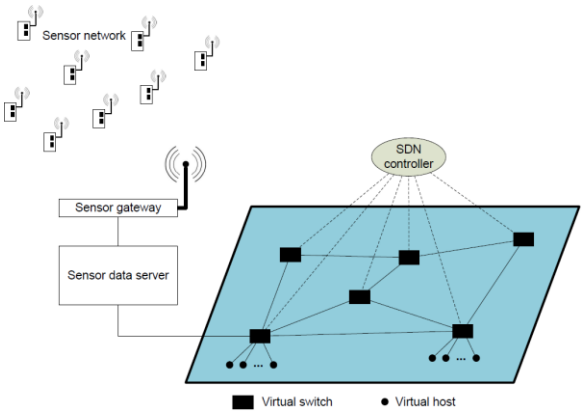

Fig. 1: The proposed experimentation architecture

The abovementioned techniques represent recent advancement in raising the security bar for the protection of NCI. Nevertheless, research concerning SDN is in an embryonic state and to the best of our knowledge the experimentation technique presented in this paper is the first reported approach to combine different capabilities and enabling conducting experiments with NCI and SDN.

3. Proposed approach for enabling SDN experiments with NCI

An emerging trend in traditional IP networks is the replacement of local router-based decision solutions with global routing decision solutions. A well-recognized enabler of this technique is OpenFlow, a protocol designed to ensure remote access to the forwarding pane of a network switch. This way, separation of control from forwarding is achieved, and more complex traffic management techniques can be implemented. OpenFlow can also bridge the gap between different network switch/router providers since the same protocol can be used to program a wide range of OpenFlow-enabled hardware devices.

Software-Defined Networking (SDN) [13] provides the means to create virtual networking services and to implement global networking decisions. It relies on OpenFlow to enable communication with remote devices and has been recently categorized as the "Next Big Technology", which will revolutionize the way decisions are implemented in switches and routers. SDN provides a directly programmable network that is managed centrally, can be monitored and configured remotely, and it is based on open standards. Therefore, OpenFlow and SDN can be seen as the technologies which provide the next generation networking capabilities for Smart Grid. These can be integrated and used in the implementation of more reliable and dynamic networking solutions, which could be also coupled with monitoring systems such as Intrusion/Anomaly Detection Systems in order to

close an important loop.

Based on the experimental capabilities offered by OpenFlow and SDN we propose an architecture which combines the effective power of software-defined network topology construction with the physical properties of critical infrastructures. The proposed architecture is shown in Fig. 1.

The experimentation network is recreated through an emulated approach by using the Mininet platform [11], [9]. Mininet provides capabilities to emulate a "network in a laptop" by using virtualization capabilities of modern Operating Systems: process name spaces are used to group host-based processes together; virtual network interfaces provide communication capabilities with hosts inside the emulated network, as well as with real hosts outside the emulation domain; Open vSwitch (OVS) comes preinstalled in Mininet and provides a realistic recreation of switching capabilities.

In terms of SDN controllers in the literature we find several such controller implementations: NOX, POX, Beacon, Floodlight, and OpenDaylight. Most of the available open controllers provide basic controller functionalities. However, in case network topologies exhibit loops and require the injection of static flows to work together with such loops, few of the controllers are able to satisfy these constraints. Subsequently, controllers must be easily programmable, they must expose an interface to communicate with real OpenFlow-enabled switches and they must support experiments with large networks as well.

Therefore, the adopted approach relies on Floodlight as an SDN controller enabler. The controller monitors the network and can take decisions in order to re-route traffic, to drop packets and to run complex traffic engineering algorithms.

On the other hand, communications with the physical domain is handled through a *Sensor data server* which collects data from *Sensor gateway* and forwards it on request to clients connected to the emulated network. An important aspect that should be mentioned at this point is that the software and protocols running on top of the emulated network are realistic and therefore they are capable to interact with each-other. This leads to the establishment of a complex environment where communications are routed over an emulated network and specific software components are running in the context of real operating systems.

Subsequently, this enables the integration of real communications originating from sensor networks. Since a major aspect of NCI is the actual gathering of data from sensor networks spread across a large area, the approach couples the two domains through the *Sensor data server*. This component plays the role of data gateway between the sensor network and the emulated network.

The main advantage of the approach is that it provides a flexible way to experiment with different traffic engineering algorithms as well as different network topologies. The approach is well suited to test the behavior of industrial protocols while routing is performed in an SDN-enabled environment.

4. Experimental results

In order to illustrate the applicability of the approach in cyber security experiments we created the setup presented in Fig. 2.

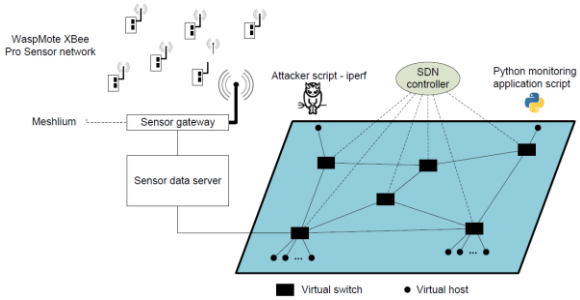

Fig. 2: Experiment setup

The sensor network consists of several *WaspMote* sensor nodes equipped with XBee Pro communication modules. Each WaspMote node transmits the measured temperature and battery level to the sensor gateway implemented with a *Meshlium* gateway. Meshlium collects the data and stores it in a local MySQL database. From there, the data is periodically read by the sensor data server which exposes an XMPP interface to enable communication with client applications.

A client application was developed in Python language which communicates with the sensor data server through a Mininet network supervised by an SDN controller. A synthetic attack was implemented with the *iperf* tool. The attack flooded the network with UDP packets which lead to the disturbance of communications and regular monitoring traffic. All network links have been limited to 1Mbit/sec.

As shown in Fig. 3 and Fig. 4 once the attack is launched it pushes the traffic throughput up to the link capacity. This leads to significant disturbance of the regular XMPP/TCP traffic, which is more visible in Fig. 5 and Fig. 6.

Once the attack is started the regular traffic experiences significant loss and delay. Nevertheless, once the attack stops, TCP protocol is able to restore normal traffic throughput by sending at first a large burst of delayed packets, significantly visible in Fig. 5 and Fig. 6.

This experiment has shown that cyber security experiments with complex systems such as large-scale NCI are possible through the approach presented in this paper. The technique constitutes the first steps towards a comprehensive framework that closes the loop between monitoring, intrusion/anomaly detection systems and mitigation measures.

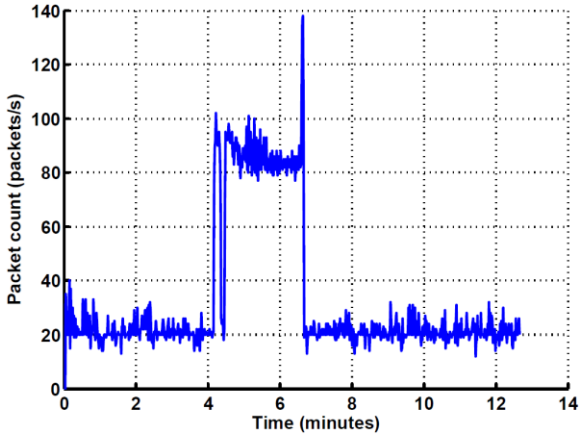

Fig. 3: Normal (XMPP/TCP) and attack traffic (Iperf/UDP) packet count

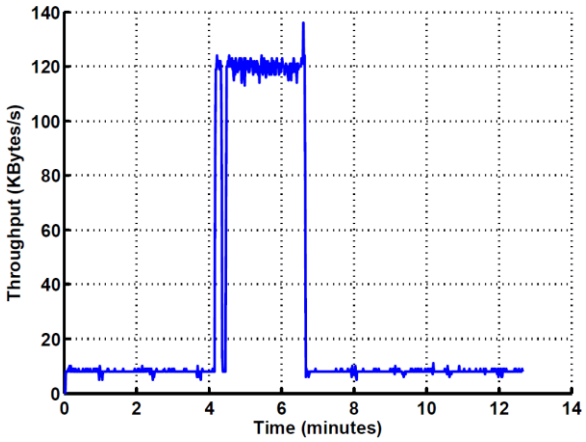

Fig. 4: Normal (XMPP/TCP) and attack traffic (Iperf/UDP) throughput

5. Conclusions

This paper demonstrated that experiments with Software Defined Networking in the context of Networked Critical Infrastructures can be conducted by adopting open source technologies such as Mininet, Floodlight, Iperf, and XMPP. Such techniques are necessary since more and more sensors are being integrated into our social lives every day. The data gathered from these sensors needs to be transported and stored in specific places across large-scale distributed communication networks. In this context novel technologies based on SDN are being accepted and deployed for this purpose, due to their many advantages.

Therefore, we consider that the technique proposed in this paper constitutes a significant progress in the unification of the two worlds: the cyber and the physical dimensions of NCI. Furthermore, we consider that the experiments presented in this paper illustrate the important impact of cyber attacks on normal communications. As future work we intend to evaluate different strategies in mitigating cyber attacks and to identify novel techniques to close a significant loop in cyber security: the loop between monitoring/detection and the actual mitigation of attacks.

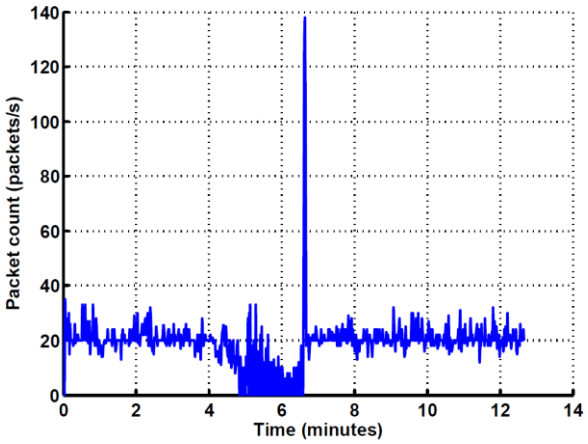

Fig. 5: Filtered normal (TCP) traffic: effect of attack on regular packet count

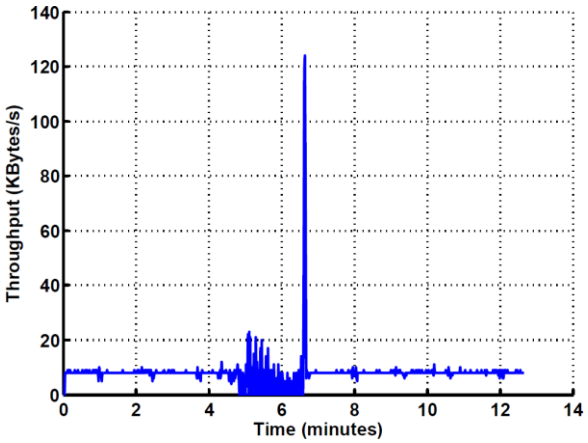

Fig. 6: Filtered normal (TCP) traffic: effect of attack on regular traffic throughput

Acknowledgement

This work was supported by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project has been supported by the European Union, co-financed by the European Social Fund.

References

[1] Bodenheim, R., Butts, J., Dunlap, S. and Mullins, B. (2014), *Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices*, International Journal of Critical Infrastructure Protection, vol. 7, no. 2, pp. 114–123.

[2] Chen, T. and Abu-Nimeh, S. (2011), *Lessons from Stuxnet*, Computer, vol. 44, no. 4, pp. 91–93.

[3] European Commission (2004). *Communication from the Commission to the Council - Critical Infrastructure Protection in the fight against terrorism*. COM(2004)0702., October 2004.

[4] Garitano, I., Siaterlis, C., Genge, B., Uribeetxeberria, R. and Zurutuza, U. (2012), *A method to construct network traffic models for process control systems*, In Emerging Technologies Factory Automation (ETFA), 2012 IEEE 17th Conference on, pp. 1-8.

[5] Genge, B. and Siaterlis, C. (2013), *Analysis of the Effects of Distributed Denial-of-Service Attacks on MPLS Networks*, International Journal of Critical Infrastructure Protection, Elsevier, vol. 6, no. 2, pp. 87-95.

[6] Genge, B., Siaterlis, C. and G. Karopoulos (2013), *Data fusion-based anomaly detection in networked critical infrastructures*, In Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on, pp. 1-8.

[7] Goldenberg, N. and Wool, A. (2013), *Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems*, International Journal of Critical Infrastructure Protection, vol. 6 no. 2, pp. 63-75.

[8] Guernsey, D., Rice, M. and Shenoi, S. (2012), *Implementing novel reactive defense functionality in MPLS networks using hyperspeed signalling*, International Journal of Critical Infrastructure Protection, vol. 5, no. 1, pp. 40–52.

[9] Handigol, N., Heller, B., Jeyakumar, V., Lantz, B. and McKeown, N. (2012), *Reproducible network experiments using container-based emulation*, Proceedings of the 8th international conference on Emerging networking experiments and technologies, pp. 253-264.

[10] Jaradat, R.M. and Keating, C.B. (2014), *Fragility of oil as a critical infrastructure problem*, International Journal of Critical Infrastructure Protection, vol 7, no. 2, pp. 86–99.

[11] Lantz, B., Heller, B. and McKeown, N. (2010), *A network in a laptop: rapid prototyping for software-defined networks*, Proceeding Hotnets-IX Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Article No. 19.

[12] National Institute of Standards and Technology (2011), *Guide to Industrial Control Systems (ICS) Securit*", NIST Special Publication 800-82.

[13] Open Networking Foundation (2014), Software-Defined Networking (SDN) Definition. [Online]. Available: https://www.opennetworking.org/sdn-resources/sdn-definition.

[14] Schuster, F., Paul, A. and H. Konig (2013), *Towards learning normality for anomaly detection in industrial control networks*, In Emerging Management Mechanisms for the Future Internet, volume 7943 of Lecture Notes in Computer Science, pp. 61-72.

[15] Weiss, J. (2010), *Protecting Industrial Control Systems from Electronic Threats*, New York, Momentum Press, May 2010.

[16] Zhao, J., Liu, K., Wang, W. and Liu, Y. (2014), *Adaptive fuzzy clustering based anomaly data detection in energy system of steel industry*, Information Sciences, vol. 259, pp. 335-345.